

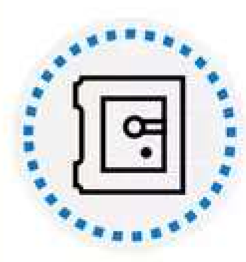
SC-900T00-A Module 4: Describe the Capabilities of Microsoft Compliance Solutions

Module Agenda


Describe the compliance management capabilities in Microsoft


Describe information protection and governance capabilities of Microsoft 365


Describe insider risk capabilities in Microsoft 365


Describe eDiscovery, & audit capabilities in Microsoft 365


Describe resource governance capabilities in Azure

Lesson 1: Describe the compliance management capabilities in Microsoft



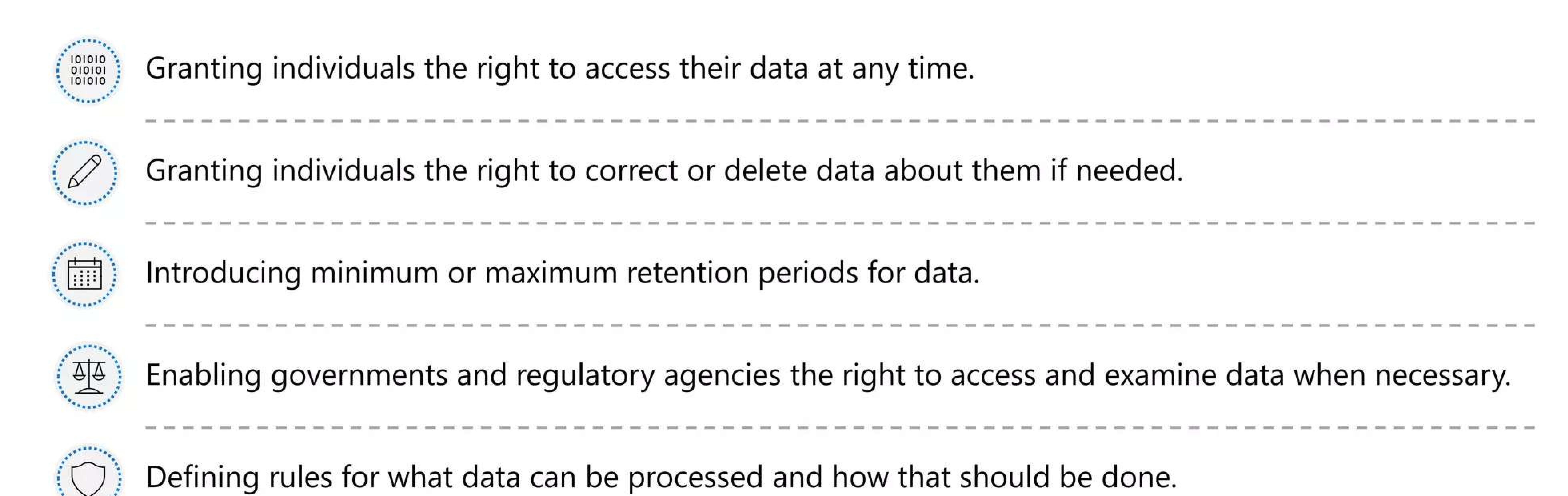
Lesson 1 Introduction

After completing this module, you should be able to:

- Describe the benefit of the Service Trust Portal.
- Describe Microsoft’s privacy principles.
- Explore the Microsoft 365 compliance center.
- Describe the benefits of Compliance Manager.

Common compliance needs

Several measures to protect data:



Service Trust Portal

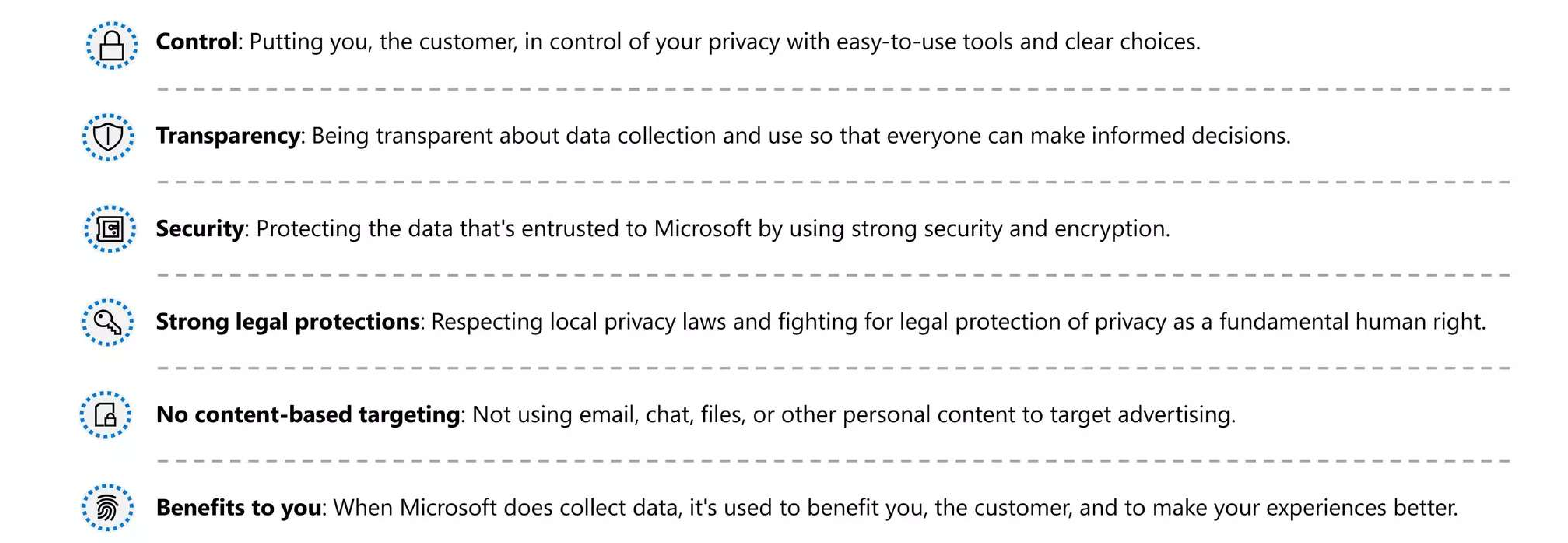
The Service Trust Portal provides:

- Information
- Tools
- Other resources about Microsoft security, privacy, and compliance practices.

You can access below offerings:

- Service Trust Portal
- Compliance Manager
- Trust Documents
- Industries & Regions
- Trust Center
- Resources
- My Library

Microsoft's privacy principles





Demo

Service Trust Portal

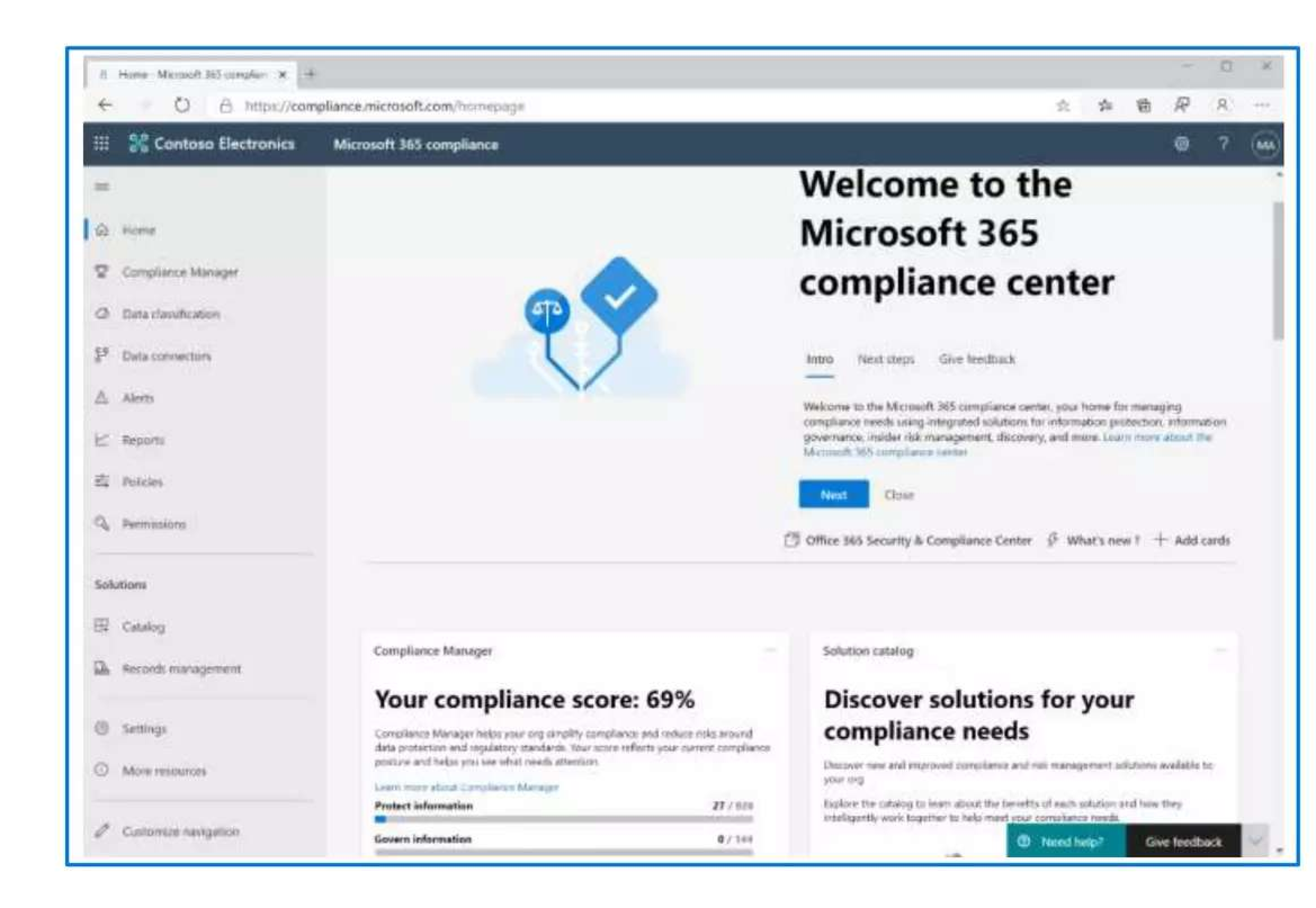
Microsoft 365 Compliance Center

Microsoft 365 Compliance center portal

- A view of how the organization is meeting its compliance requirements
- Solutions that can be used to help with compliance
- Information about active alerts
- And more…

Navigation

- Access to alerts, reports, policies, compliance solutions, and more.
- Add or remove options for a customized navigation pane.
- Customize navigation control.



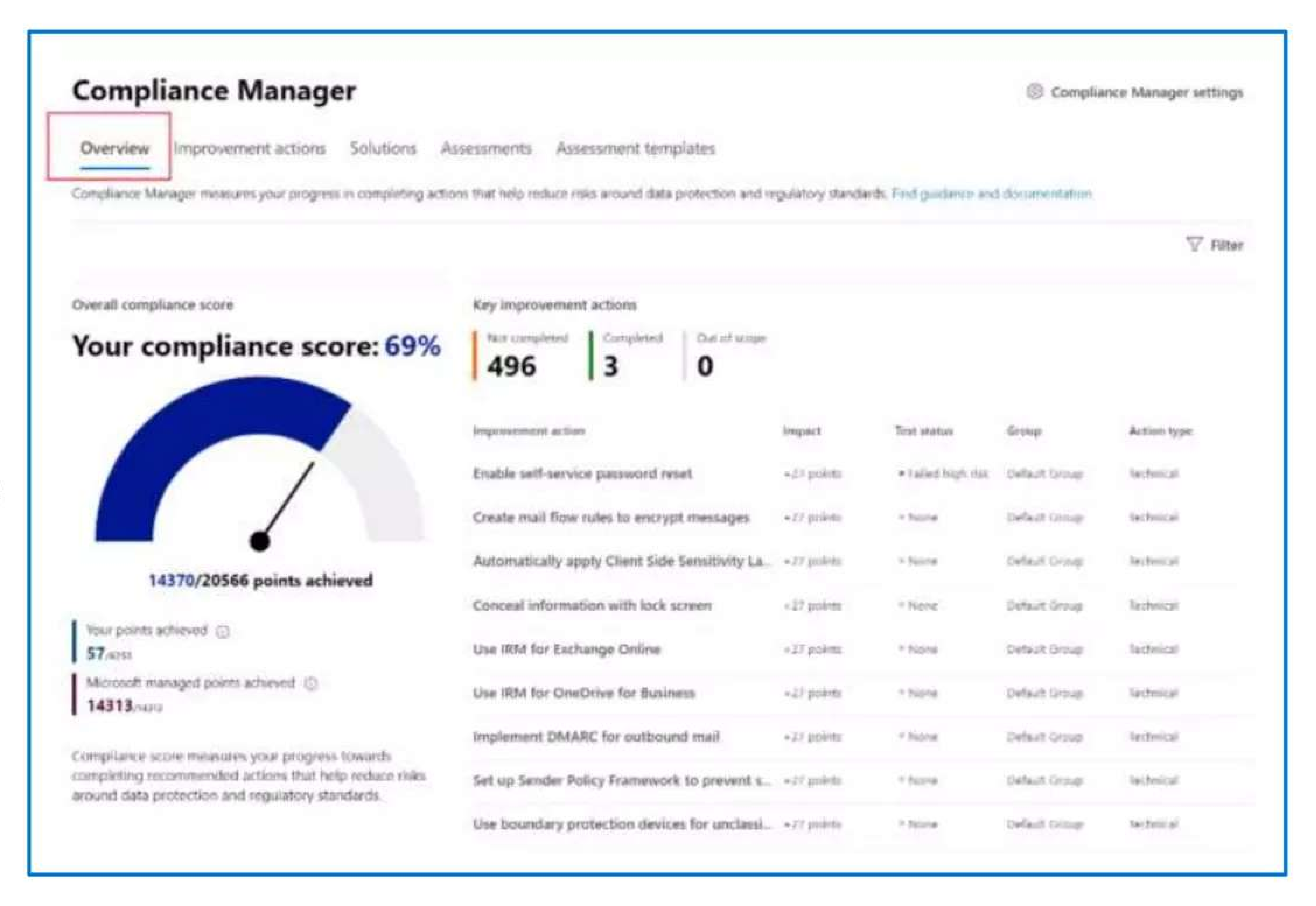
Compliance Manager

Compliance Manager simplifies compliance and reduces risk by providing:

- Prebuilt assessments based on common standards
- Workflow capabilities to complete risk assessments
- Step-by-step improvement actions
- Compliance score, shows overall compliance posture

Key elements of Compliance Manager

- Controls
- Assessments
- Templates
- Improvement actions



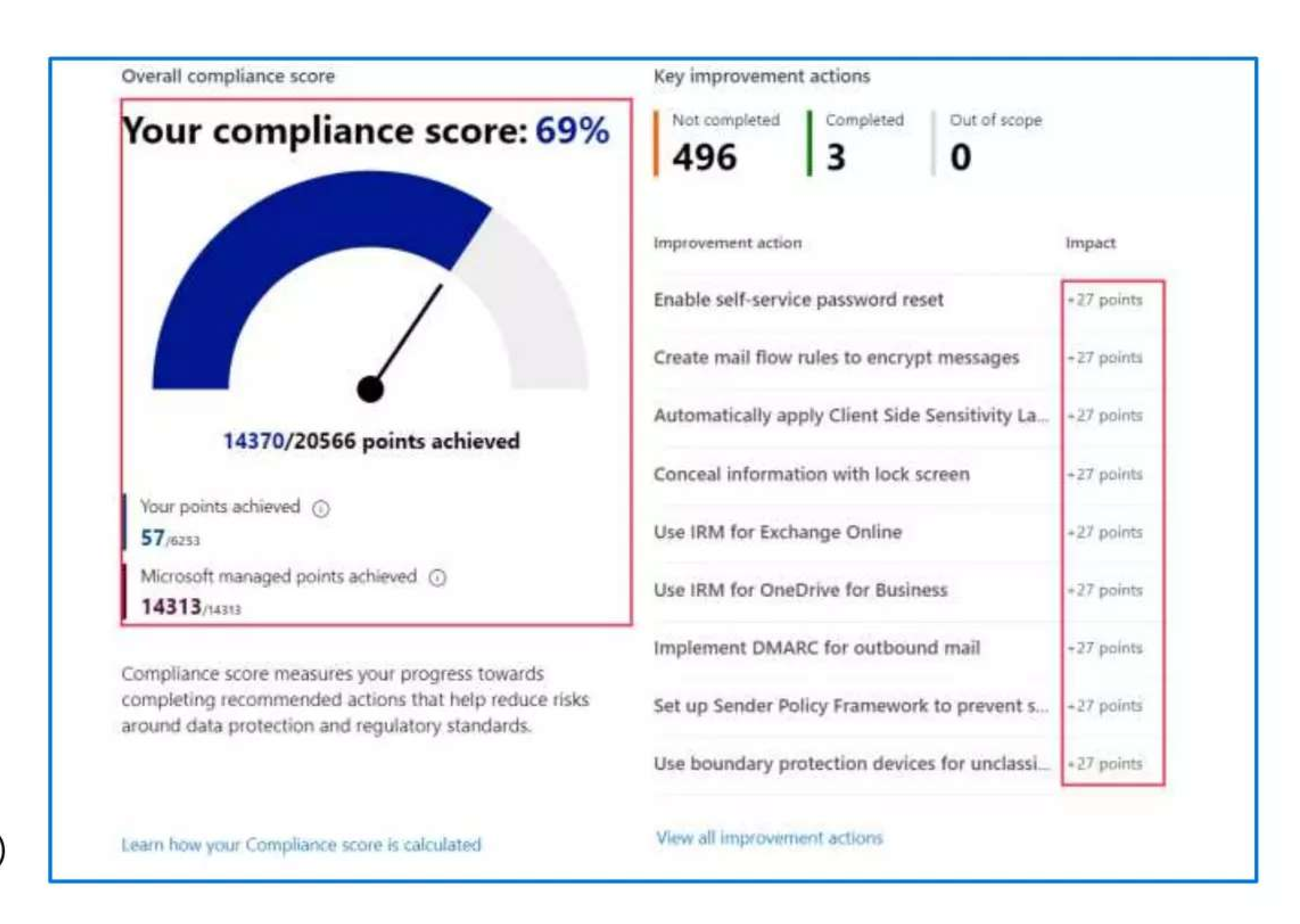
Compliance score

Benefits of compliance score:

- Help an organization understand its current compliance posture.
- Help prioritize actions based on their potential to reduce risk.

Understand your compliance score

- Actions
  - Your improved actions
  - Microsoft actions
- Action types (& action subcategory)
  - Mandatory (preventive, detective, or corrective)
  - Discretionary (preventive, detective, or corrective)





Demo

Microsoft 365 Compliance Center

Lesson 2: Describe information protection and governance capabilities of Microsoft 365



Lesson 2 Introduction

After completing this module, you should be able to:

- Describe data classification capabilities.
- Describe records management.
- Describe data loss prevention.

Know your data, protect your data, and govern your data



Know your data: Understand your data landscape and identify important data across on-premises, cloud, and hybrid environments.



Protect your data: Apply flexible protection actions including encryption, access restrictions, and visual markings.



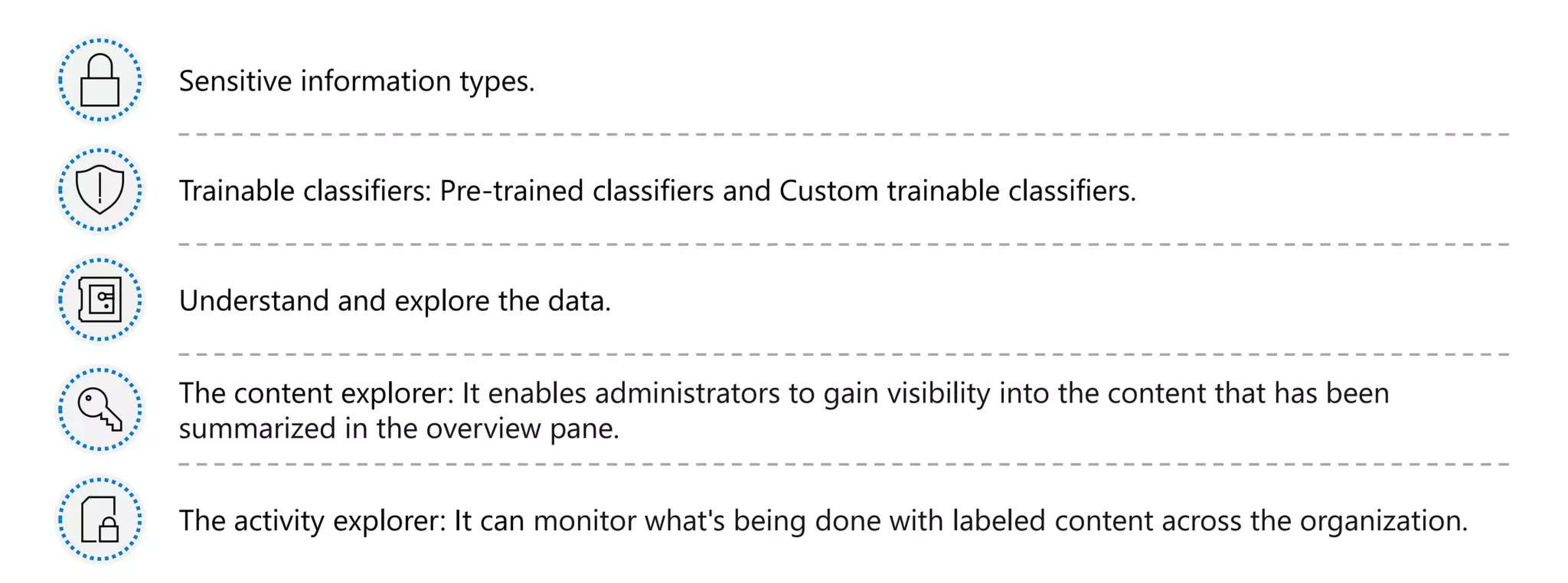
Prevent data loss: Detect risky behavior and prevent accidental oversharing of sensitive information.



Govern your data: Automatically keep, delete, and store data and records in a compliant manner.



Data classification capabilities in the Microsoft 365 Compliance Center



Sensitivity labels and policies

Sensitivity labels

Labels are:

- Customizable
- Clear text
- Persistent

Usage:

- Encrypt email and documents.
- Mark the content.
- Apply the label automatically.
- Protect content in containers: sites and groups.
- Extend sensitivity labels to third-party apps and services.
- Classify content without using any protection settings.

Label policies

Policies enable admins to:

- Choose the users and groups that can see labels
- Apply a default label to all new emails and documents
- Require justifications for label changes
- Require users to apply a label (mandatory labeling)
- Link users to custom help pages

Once a sensitivity label is applied to an email or document, any configured protection settings for that label are enforced on the content.



Demo

Sensitivity labels

Describe data loss prevention (DLP)

DLP protects sensitive information and prevents its inadvertent disclosure.

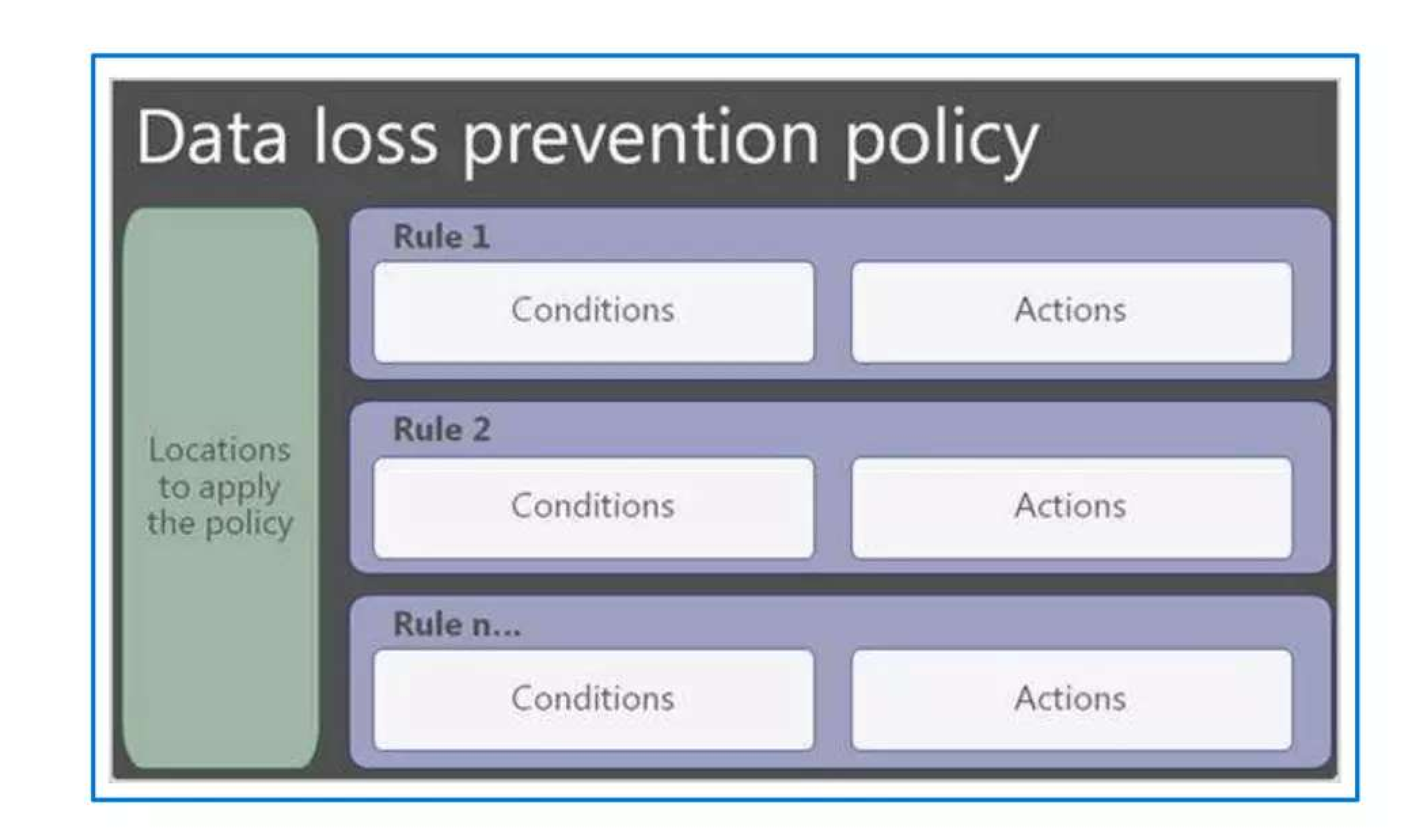
- DPL policies protect information by identifying and automatically protecting sensitive data.
- Protect sensitive information across Microsoft 365 – OneDrive for Business, SharePoint Online, Exchange Online and Microsoft Teams

Endpoint Data Loss Prevention

- DLP extended to Windows 10 devices.
- Audit and manage activities including creating, coping, printing, & renaming items

Data Loss Prevention in Microsoft Teams

- DPL capabilities extended to Microsoft Teams chat and channel message.



Retention labels and policies

Retention settings work with SharePoint, OneDrive, Teams, Yammer and Exchange and help organizations manage and govern information by ensuring content is kept only for a required time, and then permanently deleted.

Retention labels:

- Are applied at an item level.
- Emails and documents can have only a single retention label assigned to it at a time.
- Retention settings from retention labels travel with the content in your Microsoft 365 tenant.
- Can be applied manually or automatically.
- Retention labels support disposition review of the content before it's permanently deleted.

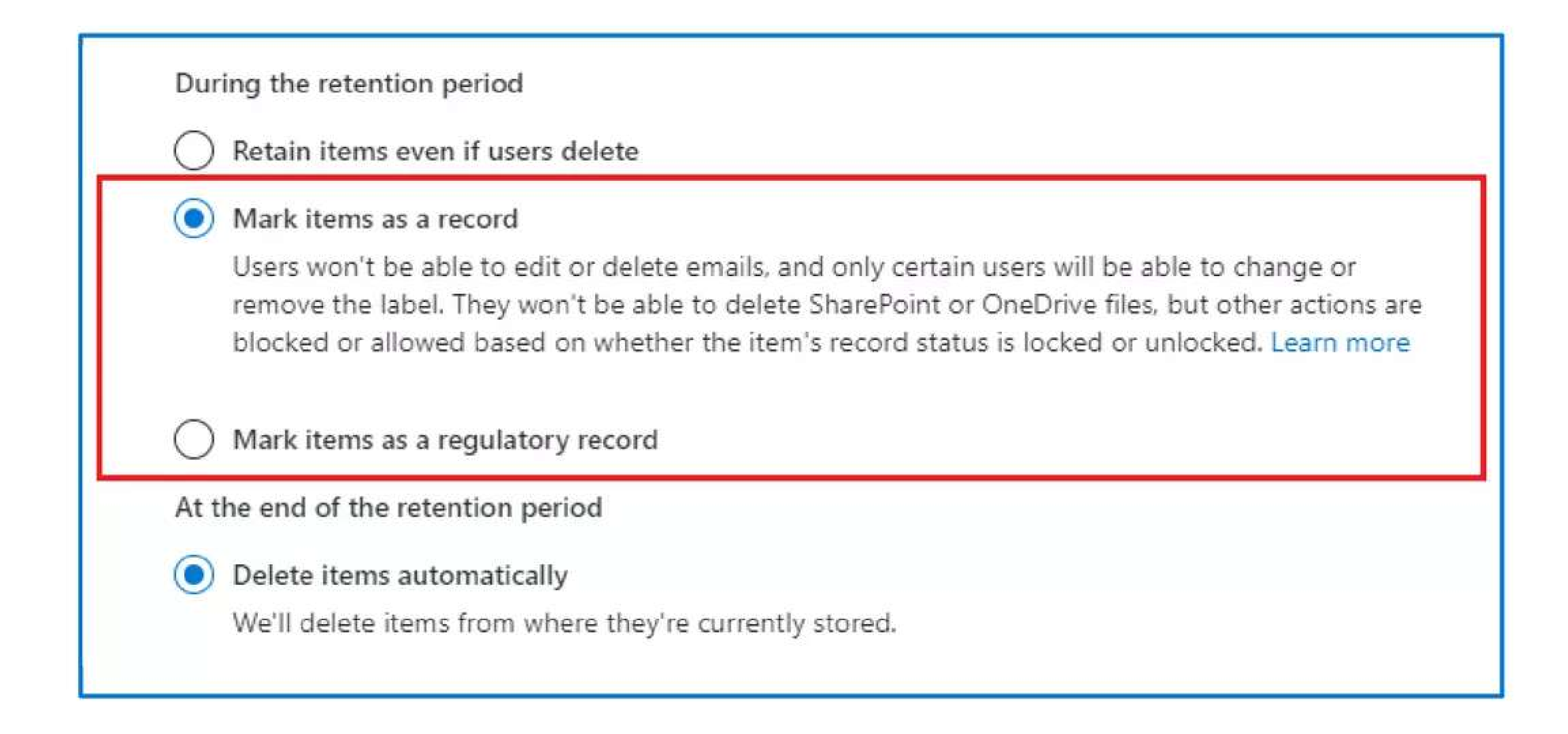
Retention policies:

- Are applied at site or mailbox level,
- Can be applied to multiple locations or specific locations or users.
- Items inherit the retention settings from their container.
- If an item is moved, the retention setting does not travel to the new location.

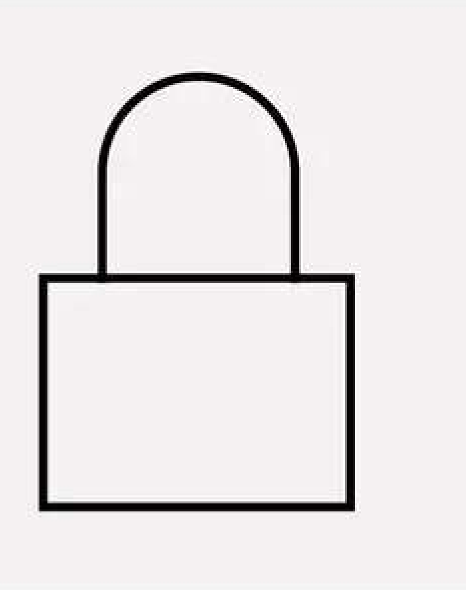
Records management

Records management in Microsoft 365 helps an organization look after their legal obligations and helps to demonstrate compliance with regulations.

- When content is labeled as a record, the following happens:
  - Restrictions are put in place to block certain activities.
  - Activities are logged.
  - Proof of disposition is kept at the end of the retention period.
- To enable items to be marked as records, an administrator sets up retention labels.



Lesson 3: Describe insider risk capabilities in Microsoft 365



Lesson 3 Introduction

After completing this module, you should be able to:

- Describe how Microsoft 365 can help organizations identify insider risks and take appropriate action.

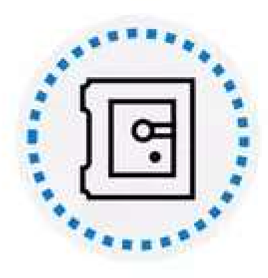
Insider risk solutions in Microsoft 365 (Slide 1)



Insider risk management helps minimize internal risks by enabling you to detect, investigate, and act on malicious and inadvertent activities in your organization.



Communication compliance helps minimize communication risks by helping you detect, capture, and act on inappropriate messages in your organization. Supported services: Microsoft Teams, Exchange Online, Yammer, & 3rd party communications in an org.



Information barriers allow you to restrict communication and collaboration between two internal groups to avoid a conflict of interest from occurring in your organization. Supported in Microsoft Teams, OneDrive for Business, SharePoint Online, and more.

Insider risk solutions in Microsoft 365 (Slide 2)

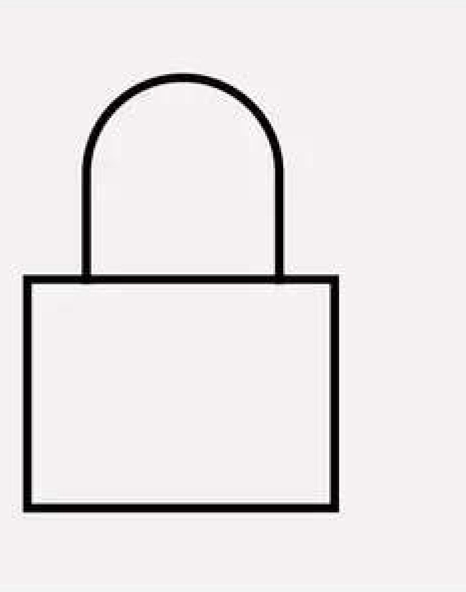


Privileged access management allows granular access control over privileged Exchange Online admin tasks in Office 365.



Customer Lockbox ensures that Microsoft cannot access customer content to perform a service operation without the customer's explicit approval. Supported services: Exchange Online, SharePoint Online, OneDrive for Business.

Lesson 4: Describe eDiscovery & Audit capabilities in Microsoft 365



Lesson 4 Introduction

After completing this module, you should be able to:

- Describe the purpose of eDiscovery & the capabilities of the content search tool.
- Describe the core & advanced eDiscovery workflows.
- Describe the core and advanced audit capabilities of Microsoft 365.

eDiscovery & content search

Purpose of eDiscovery

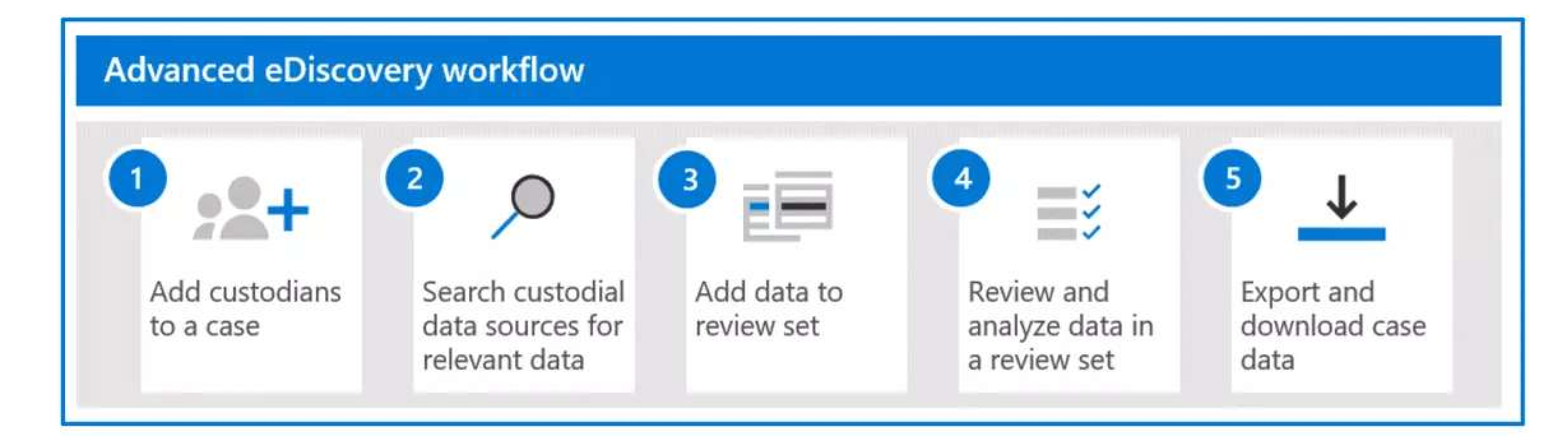
- Find electronic information to be used as evidence when a company is involved in litigation..
- Search for content in Exchange Online mailboxes, Microsoft 365 Groups, Microsoft Teams, SharePoint Online and OneDrive for Business sites, Skype for Business conversations, and Yammer teams.
- Use to identify, hold, and export content found in mailboxes and sites.

Content Search

- Search Exchange Online mailboxes, SharePoint Online sites, OneDrive for Business, Teams, Microsoft 365 groups, Yammer groups
- Build search queries and use conditions
- Create, report on, and delete multiple searches
- View keyword statistics
- Search for third-party data
- PowerShell scripts for more complex search related tasks

Core and advanced eDiscovery workflows





Core eDiscovery

1. Create a hold to preserve content that might be relevant to the case (mailboxes, sites, and public folders).
2. Create and run searches for content that relates to the case.
3. Export and download search results.

Advanced eDiscovery builds on core eDiscovery

1. Add persons of interest (custodians) and data sources that aren't associated with a specific user.
2. Use the built-in collections tool to search data sources for content relevant to the case.
3. Data added to a review set are copied from their original location to a secure Azure Storage location. The data is reindexed again to optimize for fast searches
4. Use a wide-variety of tools and capabilities to view and analyze the case data with goal of reducing the data set to what is most relevant to the case
5. Export and download case data

Audit capabilities of Microsoft 365

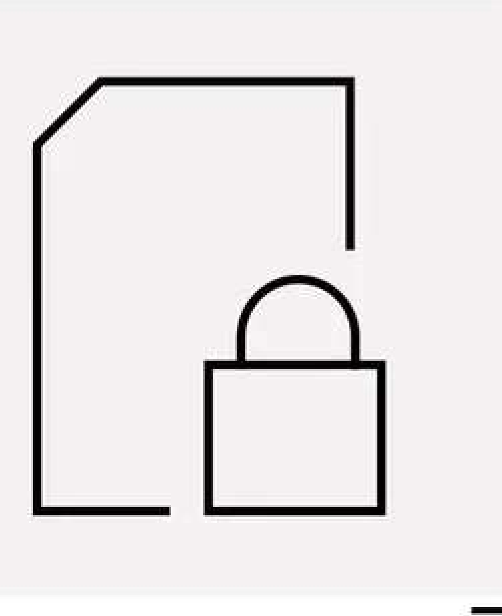
Core Audit

- Allows organizations to view user and administrator activity.
- An audited activity generates an audit record that is stored in the audit log.
- Searching the audit log requires the search capability to be turned on and assigned the appropriate role.
- The results can be filtered and exported to a CSV file.

Advanced Audit - Core Audit, plus:

- Long-term retention of audit logs
- Customized audit retention policies
- High-bandwidth access to Office 365 Management Activity API
- Access to crucial events for investigations
  - MailItemsAccessed
  - Send
  - SearchQueryInitiatedExchange
  - SearchQueryInitiatedSharePoint

Lesson 5: Describe resource governance capabilities in Azure



Lesson 5 Introduction

After completing this module, you should be able to:

- Describe some of the resource governance capabilities in Azure.

Azure Resource Manager locks

Azure Resource Manager locks

- Prevent resources from being accidentally deleted or changed.
- Apply a lock at a parent scope, all resources within that scope inherit that lock.
- Apply only to operations that happen in the management plane.
- Changes to the actual resource are restricted, but resource operations aren't restricted.

A lock level

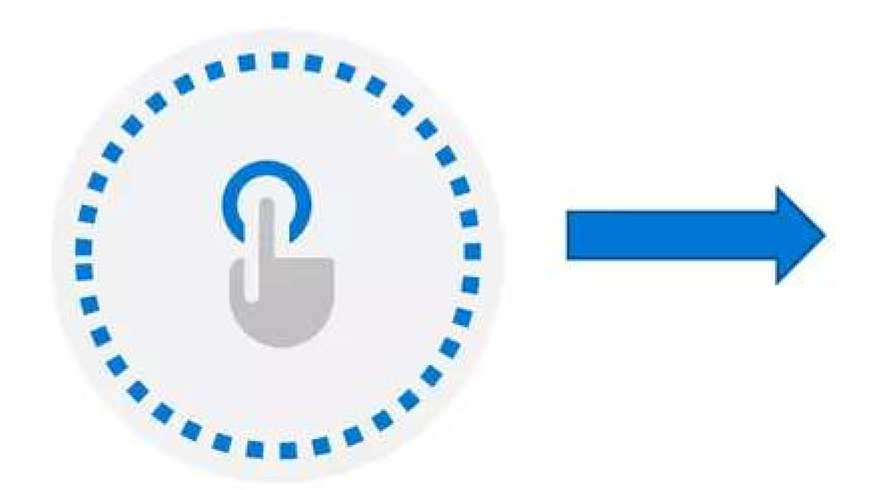
- CanNotDelete
- ReadOnly

Azure Blueprints

- Azure Blueprints provide a way to define a repeatable set of Azure resources.
- Rapidly provision environments, that are in line with the organization's compliance requirements.
- Provision Azure resources across several subscriptions simultaneously for quicker delivery.
- Declarative way to orchestrate the deployment of various resource templates and artifacts, including:
  - Role Assignments
  - Policy Assignments
  - Azure Resource Manager templates (ARM templates)
  - Resource Groups
- Blueprint objects are replicated to multiple Azure regions.
- The relationship between the blueprint definition and the blueprint assignment is preserved.

Azure Policy

Trigger a Policy evaluation

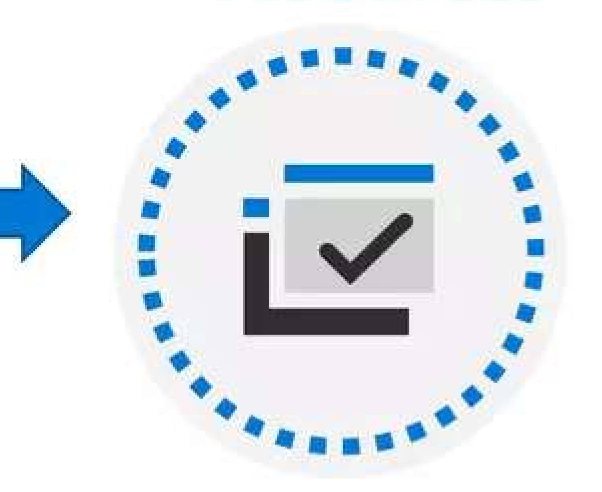


- In-scope resource is created, deleted, or updated
- A policy or an initiative is newly assigned to a scope.
- A policy or an initiative assigned to a scope is updated.
- The standard compliance evaluation cycle

Azure Policy

- Help enforce standards and assess compliance across your organization.
- A compliance dashboard, to evaluate the overall state of the environment.
- Evaluates resources in Azure and Arc enabled resources.

Responses to non-compliant resources



- Deny a change to a resource.
- Log changes to a resource.
- Alter a resource before or after a change.
- Deploy related compliant resources.



Demo

Azure policy

Module Summary

In this lesson, you have:

- Learned about the compliance management capabilities in Microsoft, including the Service Trust Portal, Microsoft 365 compliance center, Microsoft privacy principles, and more.
- Learned about the information protection and governance capabilities of Microsoft 365, including sensitivity & retention labels, DLP, and more.
- Learned about insider risk capabilities in Microsoft 365
- Learned about eDiscovery & audit capabilities of Microsoft 365
- Describe resource governance capabilities in Azure, including Azure policy, resource locks, Blueprints, and more.


Microsoft Security